Cybersecurity als integraler Bestandteil von Gebäudeplanung und -betrieb

Smart Buildings ermöglichen eine zentrale Steuerung, automatisierte Abläufe und eine effiziente Ressourcennutzung. So lassen sich der Betrieb vereinfachen, Kosten senken und die Nachhaltigkeit verbessern. Doch die zugrundeliegende Vernetzung eröffnet gleichzeitig neue Angriffsflächen für Cyber-Kriminelle.

Autoren:
Hauke Kästing
Leitung Industrial Security im Vertikal Market Management
Phoenix Contact Deutschland GmbH, Blomberg

Frank Schröder
Leitung Technology Integration (R&D) im Corporate Facility Management
Phoenix Contact GmbH & Co. KG, Bad Pyrmont

Christina Süß
Leitung Software Systems im Corporate Facility Management
Phoenix Contact GmbH & Co. KG, Bad Pyrmont

Mehr Informationen:
www.phoenixcontact.de/gebaeude

Die Bedrohungen von Smart Buildings erweisen sich als vielfältig. Sie reichen vom Datendiebstahl und Phishing-Angriffen bis zu Denial-of-Service-Attacken und Ransomware. Besorgniserregend ist die Möglichkeit, dass Cyber-Kriminelle die Kontrolle über kritische Systeme eines Gebäudes übernehmen können. Neben finanziellen Verlusten und physischen Schäden kann es somit zu Sicherheitsrisiken kommen. Aufgrund der wachsenden Bedrohungslage zeigt es sich daher als unerlässlich, Cybersecurity von Anfang an als integralen Bestandteil der Gebäudeplanung und des -betriebs zu betrachten. Das umfasst nicht nur den Schutz der physischen Infrastruktur, sondern auch die Absicherung der digitalen Systeme durch Verschlüsselung, Zugriffskontrollen und regelmäßige Sicherheits-Updates.

Klar definierte Reaktionspläne und umfassende Schulungen

Abgesehen von der Abwehr möglicher Angriffe müssen Betreiber auf den Ernstfall vorbereitet sein – technisch wie organisatorisch. Dabei bildet ein wirksames Risikomanagement die Grundlage. Tritt ein Sicherheitsvorfall auf, ist dessen schnelle und koordinierte Behandlung notwendig. Dazu gehören klar definierte Reaktionspläne, um den Schaden einzugrenzen und den Angreifer möglichst rasch zu erkennen und zu isolieren. Parallel muss die Aufrechterhaltung des Betriebs sichergestellt sein. Ein Backup-Management und Wiederherstellungsstrategien tragen zu einer zügigen Rückkehr zum Normalbetrieb bei. Ein Krisenmanagement rundet das Konzept ab, indem es Kommunikationsabläufe, eine Entscheidungsfindung sowie die Nachbereitung kritischer Situationen vorgibt.

Ohne Frage steht und fällt ein wirksames Cybersecurity-Konzept mit den Menschen, die es realisieren. Deshalb erweisen sich Schulungen zur Informationssicherheit als wichtig, damit die Mitarbeitenden für Bedrohungen wie Phishing, Social Engineering oder unsichere Passwörter sensibilisiert sind. Eine ebenso große Bedeutung kommt der Sicherheit des Personals zu. Hierzu zählen Zugriffskontrolllösungen, sodass lediglich befugte Personen die kritischen Systeme steuern können. Darüber hinaus sollte das Anlagen-Management physische Sicherheitsmaßnahmen wie Zutrittskontrollen und eine Überwachung des Gebäudes beinhalten. Authentifizierungslösungen schützen zusätzlich vor unbefugten Zugriffen. Darunter fallen starke Passwörter und eine

Das Gebäudemanagementsystem Emalytics bietet eine Lösung, die IO und IT im Schaltschrank zusammenführt. Das ermöglicht eine effiziente Integration und Verwaltung von Daten und Prozessen.

Für ein erfolgreiches ISMS ist die Awareness der Mitarbeitenden ein wichtiger Baustein. Sie müssen nicht nur sensibilisiert werden, eine gute Weiterbildung erweist sich ebenfalls als essenziell.

Multi-Faktor-Authentifizierung. Zudem sollte die Sprach-, Video- und Textkommunikation abgesichert werden, um sensible Informationen im Krisenfall zuverlässig und abhörsicher austauschen zu können. Ergänzend ist die systematische Nutzung von Kryptografie und Verschlüsselung in den Alltag zu integrieren.

Inventarisierung der Assets und Begrenzung der Angriffspunkte

Es ist wesentlich, zu wissen, welche IP-basierten Geräte im Facility-Netzwerk installiert sind und wie diese untereinander Daten weiterleiten. Die Assets müssen inventarisiert werden. Die Verantwortung dafür obliegt dem Facility Management. Dabei sollten die wichtigsten Merkmale der Geräte aufgeführt werden, zum Beispiel deren Verortung sowie die Hardware- oder Firmware-Revisionsstände. Ist der Status der netzgebundenen Geräte nicht sichtbar, kann dies die Cyber Security beeinträchtigen. Kompromittierte oder defekte Komponenten können zu unerwarteten Maschinenoperationen führen und somit Sicherheitsrisiken darstellen.
Eine Netzwerksegmentierung zur Trennung bei Cyber-Angriffen zeigt sich als sinnvoll, denn dem Angreifer wird ein deutlich geringeres Angriffsspektrum geboten. Die Anforderungen an ein Netzwerk- und Firewalling beinhalten sowohl technische als auch organisatorische Aspekte, die eine enge Verknüpfung zur IT bedürfen. Je nach vertikalem Segment ist entweder die IT oder OT für den Betrieb der Netzwerk- und Firewalling-Ausrüstung verantwortlich.
Die IT steht beim Betrieb in der Pflicht, während die OT die Zuständigkeit für Konfigurationen und Regeln hat. Bei der Aufteilung der Segmente müssen die im Netzwerk befindlichen Geräte stets bidirektional im Teilsegment kommunizieren können und teilweise darüber hinaus. In diesem Zusammenhang muss bekannt sein, welche Protokolle auf welchen Ports im Netzwerk Daten austauschen dürfen. In enger Absprache mit der IT ist die Übertragung der IP-basierten Geräte zu erlauben, damit das Building-Management-System die Komponenten steuern und regeln kann. Nicht alle im Gebäudeumfeld verwendeten Protokolle arbeiten verschlüsselt, weshalb bestimmte Firewall-Regeln notwendig sind.

Nutzung von KI zur Erkennung von Anomalien

Fällt das Netzwerk aus, laufen die Infrastrukturanlagen wie Druckluft weiter. In diesem Moment ist kein Monitoring möglich, die Steuerung der überlagerten Controller funktioniert allerdings noch. Bei einem Cyber-Angriff kann sich die Situation anders darstellen. Unter Umständen ist die Infrastruktur dann lahmgelegt. Jetzt kommt es darauf an, welche Bereiche betroffen sind. Je nachdem, wie Anlagen redundant und im Verbund aufgebaut wurden, lassen sich gegebenenfalls einzelne Anlagen manuell anschalten. IT und OT müssen nun besprechen, welche Bereiche wiederherzustellen sind und kurzfristig zur Verfügung stehen. Dabei kommen Notfall- und Recovery-Pläne im Facility-Management zum Einsatz. Anspruchsvoller gestaltet sich die Situation, wenn beispielsweise externe Unternehmen mit Wartungsaufgaben betraut werden. Deren Mitarbeitende verschaffen sich mit betriebsfremden IT-Geräten – wie Notebooks – Zugang zur Anlage, um Steuerungen auszulesen oder Updates auf die Geräte zu laden. Dieser Prozess erfordert eine gesonderte Vorgehensweise sowie die Weiterleitung entsprechender Informationen an den Wartungsdienstleister.
Das Risiko einer Cyber-Attacke durch Übertragung von Schad-Software lässt sich durch verschiedene Maßnahmen minimieren. Letztendlich gilt es eine Übersicht sämtlicher wichtigen Systeme und deren Angriffsoptionen zu validieren und Prioritäten zu setzen. An dieser Stelle helfen organisatorische und systematische Maßnahmen. Vor allem ist das Bewusstsein der Mitarbeitenden für Cybersecurity zu schärfen. Denn die unterschiedlichen Fachbereiche können dazu beitragen, die technischen Anlagen und Systeme weiter zu härten. Zu diesem Zweck wird auch KI genutzt, die Abnormalitäten im Netzwerk erkennen kann. ◄

Man kann nur schützen, was man kennt. Daher kommen dem Asset-Management und aktuellen Netzwerkplänen eine wesentliche Bedeutung für ein ganzheitliches Security-Konzept zu.